8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/753,727	01/03/2001	Rosario Gennaro	RSW920000091US1	3760

7590 08/10/2005

Gerald R. Woods
IBM Corporation T81/503
P.O. Box 12195
Research Triangle Park, NC 27709

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

47

Office Action Summary	**Application No.** 09/753,727	**Applicant(s)** GENNARO, ROSARIO	
	Examiner Matthew T. Henning	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 June 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,6,7,9-14,18,19,21-26,30-32,34-37,39,40,44,45 and 47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)□ Claim(s) *1,2,6,7,9-14,18,19,21-26,30-32,34-37,39,40,44,45 and 47* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *1/3/2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

This action is in response to the communication filed on 6/6/2005.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/6/2005 has been entered.

Response to Arguments

Applicant's arguments filed 6/6/2005 have been fully considered but they are not persuasive. Applicant argues primarily that:

a. Patel does not disclose a "C-bit exponent".

b. Patel disclosed outputting the lower n-ω(log n) bits.

c. Patel disclosed the generator "result" is n bits long.

d. Patel disclosed that in the preferred embodiment, the exponent was the entire result of the previous iteration, and not "C-bits" of the result.

e. Section 5.1 was merely a proof of security section and not a Patel's algorithm.

f. Patel referred to the size of the exponents as "large" in section 7.1.

g. Patel teaches against using short exponents.

The examiner notes the applicant's use of "result" to indicate the whole output of the bit generator, and the use of "output" to refer to the portion actually used by Patel as pseudo-random bits and will use the same terminology for consistency.

Regarding applicant's argument a., that Patel does not disclose a "C-bit exponent", the examiner does not find the argument persuasive. This is due to the following reason, as well as the responses to applicant's arguments b-g. Patel states on page 307 Section 2.1 Lines 1-2 that *"for efficiency purposes the exponent x is sometimes restricted to c bits (e.g. c=128 or 160 bits) since this requires fewer multiplications.*" Patel goes on to state in lines 1-3 of the following paragraph that "*we will also restrict x, in particular, we will restrict it to be slightly greater than O(log n) bits, but not to save on multiplications. The size of the exponent will be denoted ω(log n)*". Quite clearly, Patel disclosed that the exponent 'x' would be restricted to "c bits" denoted "ω(log n)". As such, the examiner does not find the argument persuasive.

Regarding applicant's argument b., that Patel disclosed outputting the lower n- ω(log n) bits, the examiner is unclear as to what this argument was meant to show considering that the argument does not reflect on the size of the exponent of Patel. However, the examiner agrees that in one embodiment, Patel disclosed outputting n - ω(log n) [or 'c'] pseudo-random bits. As such, the examiner does not find the argument persuasive.

Regarding applicant's argument c., that Patel disclosed that the generator result is 'n' bits long, the examiner has considered the argument and does not find the argument persuasive. Again, the examiner is unclear as to what this argument was meant to show, considering that the argument does not reflect on the size of the exponent of Patel. As such, the examiner does not find the argument persuasive.

Regarding applicant's argument d., that Patel disclosed that the entire result of the previous iteration was used as the exponent, the examiner has considered the argument and does not find the argument persuasive. Although Patel did disclose the use of the entire result as the exponent for the next iteration, this was merely the preferred embodiment of Patel. As discussed above with regards to argument a., Patel clearly disclosed, at least for one embodiment, limiting the exponent to $\omega(\log n)$ bits, or c bits. See MPEP Section 2123

> ***PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN***
>
> *"The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)).*
>
> *A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments. Merck & Co. v. Biocraft Laboratories, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), cert. denied, 493 U.S. 975 (1989). See also Celeritas Technologies Ltd. v. Rockwell International Corp., 150 F.3d 1354, 1361, 47 USPQ2d 1516, 1522-23 (Fed. Cir. 1998) (The court held that the prior art anticipated the claims even though it taught away from the claimed invention. "The fact that a modem with a single carrier data signal is shown to be less than optimal does not vitiate the fact that it is disclosed.").* ***NONPREFERRED EMBODIMENTS CONSTITUTE PRIOR ART***
>
> *Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. In re Susi, 440 F.2d 442, 169 USPQ 423 (CCPA 1971). "A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use." In re Gurley, 27 F.3d 551, 554, 31 USPQ2d 1130, 1132 (Fed. Cir. 1994) (The invention was directed to an epoxy impregnated fiber-reinforced printed circuit material. The applied prior art reference taught a printed circuit material similar to that of the claims but impregnated with polyester-imide resin instead of epoxy. The reference, however, disclosed that epoxy was known for this use, but that epoxy impregnated circuit boards have "relatively acceptable dimensional stability" and "some degree of flexibility," but are inferior to circuit boards impregnated with polyester-imide resins. The court upheld the rejection concluding that applicant's argument that the reference teaches away from using epoxy was insufficient to overcome the rejection since "Gurley asserted no discovery beyond what was known in the art." 27 F.3d at 554, 31 USPQ2d at 1132.).*

As such, because Patel disclosed the use of "short exponents", Patel meets the limitations of the claims. As such, the examiner does not find the arguments persuasive.

With regards to applicant's argument e., that section 5.1 was merely a proof of security section and not part of the algorithm, the examiner has considered the argument and does not find the argument persuasive. See MPEP Section 2122

UTILITY NEED NOT BE DISCLOSED IN REFERENCE

> *In order to constitute anticipatory prior art, a reference must identically disclose the claimed compound, but no utility need be disclosed by the reference. In re Schoenwald, 964 F.2d 1122, 22 USPQ2d 1671 (Fed. Cir. 1992) (The application claimed compounds used in ophthalmic compositions to treat dry eye syndrome. The examiner found a printed publication which disclosed the claimed compound but did not disclose a use for the compound. The court found that the claim was anticipated since the compound and a process of making it was taught by the reference. The court explained that "no utility need be disclosed for a reference to be anticipatory of a claim to an old compound." 964 F.2d at 1124, 22 USPQ2d at 1673. It is enough that the claimed compound is taught by the reference.).*

As such, simply because section 5.1 deals with proving the security of the system, does not mean that the section is irrelevant. Section 5.1, is a section proving the security of the algorithm of section 5. As recited on page 16 Lines 13-18, Patel disclosed using short exponents as the exponents for the system. Further, as discussed above with regards to argument a., Patel clearly disclosed limiting the exponent to a short exponent. As such, the examiner does not find the argument persuasive.

Regarding the applicant's argument f., that Patel referred to the size of the exponents as "large" in section 7.1, the examiner has considered the argument and does not find the argument persuasive. The claims do not recite that the exponents are not large, only that they are shorter than the generated result. As discussed above, in one embodiment the exponent is a short exponent and as such the examiner does not find the argument persuasive.

Regarding the applicant's argument g., that Patel teaches against using short exponents, the examiner has considered the argument and does not find it persuasive. As discussed above, Patel clearly disclosed using short exponents in the system. Simply because Patel gives disadvantages to using short exponents does not take away from the fact that Patel previously disclosed the use of short exponents, and therefore met the limitations of the claims.

Furthermore, see MPEP Section 2121

PRIOR ART IS PRESUMED TO BE OPERABLE/ ENABLING

> *When the reference relied on expressly anticipates or makes obvious all of the elements of the claimed invention, the reference is presumed to be operable. Once such a reference is found, the burden is on applicant to provide facts rebutting the presumption of operability. In re Sasse, 629 F.2d 675, 207 USPQ 107 (CCPA 1980). See also MPEP § 716.07.*

Because the arguments have not been found persuasive, the examiner is maintaining the 102 rejections in view of Patel as set forth below.

DETAILED ACTION

All rejections and objections not set forth below have been withdrawn.

Claims 1-2, 6-7, 9-14, 18-19, 21-26, 30-32, 34-37, 39-40, 44-45, and 47 have been examined.

Claims 3-5, 8, 15-17, 20, 27-29, 33, 38, 41-43, and 46 have been cancelled.

Title

The title as amended is acceptable.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-2, 6-7, 9-14, 18-19, 21-26, 30-32, 34-37, 39-40, 44-45, and 47 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "substantially" in claims 1, 13, 25, and 39 is a relative term which renders the claim indefinite. The term "substantially" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. One of ordinary skill in the art would be unable to determine how much shorter a length of the input would have to be in order to be considered substantially shorter than a length of the generated output. As such, the recitation of "substantially" in this claim would cause the ordinary person to be unable to determine the scope of the claim, and as such the claims is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

Claims 1, 13, 25, and 39 recite the limitations "wherein a length in bits, C, of the input" and "a length in bits, N, of the generated output". It is unclear from the claim whether "a length" is meant as "a portion of the input/output" (i.e. the first 10 bits of the input) or whether it is meant as "the total number of bits in the input/output". As such, the ordinary person skilled in the art would be unable to determine the scope of the claim. Therefore, the claims is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

Any claim not specifically addressed above is rejected by virtue of its dependency from one of the rejected independent claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 13-14, 18-19, 21-22, 24-26, 30-32, 34-35, 37, 39-40, 44-45, and 47 are rejected under 35 U.S.C. 102(b) as being anticipated by Patel et al ("An Efficient Discrete Log Pseudo Random Generator") hereinafter referred to as Patel.

Regarding claim 13, Patel disclosed a system for efficiently generating pseudo-random bits in a computing environment, comprising: means for providing an input value (See Patel Page 313 Section 5 Line 10); means for generating an output sequence of pseudo-random bits (See Patel Page 313 Section 5 Lines 11-12) using the provided input value as an exponent of a 1-way function comprising modular exponentiation modulo a safe prime number (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i} \bmod p$ is one-way and Page 307 Paragraph 6 Lines 7-8) wherein a length in bits, C (See Patel Page 307 Section 2.1 Paragraphs 1-2, $\omega(\log n)$), of the input value is substantially shorter than a length in bits, N (See Section 5 Lines 9-10, x_{i+1}), of the generated output sequence (See Patel Page 307 Problem 2) and a base of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4), and means for using C selected bits of the generated output sequence as the provided input value for the next iteration of the means for generating (See Patel Page 307 Section 2.1 Paragraphs 1-2 and Patel Page 316 Lines 9-10) while using all N-C remaining bits of the generated output sequence as pseudo-random output bits (See Patel Page 316 Lines 5-6), until a desired number of pseudo-random output bits have been generated (See Patel section 5 Lines 9-11, wherein the feedback is performed for all $i>0$).

Regarding claim 25, Patel disclosed a method for efficiently generating pseudo-random bits, comprising: providing an input value (See Patel Page 313 Section 5 Line 10); generating an output sequence of pseudo-random bits (See Patel Page 313 Section 5 Lines 11-12) using the provided input value as an exponent of a 1-way function comprising modular exponentiation modulo a safe prime number (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i} \bmod p$ is one-way and Page 307 Paragraph 6 Lines 7-8) wherein a length in bits, C (See Patel

Page 307 Section 2.1 Paragraphs 1-2, ω(log n)), of the input value is substantially shorter than a length in bits, N (See Section 5 Lines 9-10, x_{i+1}), of the generated output sequence (See Patel Page 307 Problem 2) and a base of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4), and means for using C selected bits of the generated output sequence as the provided input value for the next iteration of the means for generating (See Patel Page 307 Section 2.1 Paragraphs 1-2 and Patel Page 316 Lines 9-10) while using all N-C remaining bits of the generated output sequence as pseudo-random output bits (See Patel Page 316 Lines 5-6), until a desired number of pseudo-random output bits have been generated (See Patel section 5 Lines 9-11, wherein the feedback is performed for all i>0).

Regarding claim 39, Patel disclosed an encryption system, comprising: means for providing an input value (See Patel Page 313 Section 5 Line 10); means for generating an output sequence of pseudo-random bits (See Patel Page 313 Section 5 Lines 11-12) using the provided input value as an exponent of a 1-way function comprising modular exponentiation modulo a safe prime number (See Patel Page 313 Section 5 Line 10 wherein the function $x_{i+1} = g^{x_i} \bmod p$ is one-way and Page 307 Paragraph 6 Lines 7-8) wherein a length in bits, C (See Patel Page 307 Section 2.1 Paragraphs 1-2, ω(log n)), of the input value is substantially shorter than a length in bits, N (See Section 5 Lines 9-10, x_{i+1}), of the generated output sequence (See Patel Page 307 Problem 2) and a base of the modular exponentiation is a fixed generator value (See Patel Page 304 Section 1 Lines 3-4), and means for using C selected bits of the generated output sequence as the provided input value for the next iteration of the means for generating (See Patel Page 307 Section 2.1 Paragraphs 1-2 and Patel Page 316 Lines 9-10) while using all N-C remaining bits of the generated output sequence as pseudo-random output bits (See Patel Page 316 Lines 5-6), until a desired number of pseudo-random output bits have been generated (See Patel section 5 Lines 9-11, wherein the feedback is performed for all i>0); and means for using the desired number of generated pseudo-random bits as input to an encryption operation (See Patel Page 305 Lines 15-17).

Regarding claims 14, 26, and 40, Patel disclosed that the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption (See Patel Page 307 Section 2.1).

Regarding claims 18, 30, and 44, Patel disclosed that the length of the input value is 160 bits (See Patel Section 2.1 Lines 1-2 wherein x is the input of 160 bits) and a length of the safe prime number is 1024 bits (See Patel Page 307 Lines 5-6).

Regarding claims 19, 31, 32, and 45, Patel disclosed that the length of the input value is at least 160 bits (See Patel Section 2.1 Lines 1-2 wherein x is the input of 160 bits) and the length of the generated output sequence is at least 1024 bits (See Patel Abstract Lines 11-13 wherein n is the number of bits output by the generator prior to bit extraction as disclosed by Patel in Section 6).

Regarding claims 21, 34, and 47, Patel disclosed that the N – C remaining bits are concatenated to pseudo-random output bits previously generated by the means for generating (See Patel Abstract and Section 7.1).

Regarding claims 22, and 35, Patel disclosed that the N – C remaining bits are selected from the N bits of the generated output sequence as a contiguous group of bits (See Patel Section 7.1 Lines 3-4).

Regarding claims 24, and 37, Patel disclosed means for using the desired number of generated pseudo-random output bits as input to an encryption operation (See Patel Page 305 Lines 15-17).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1-2, 6-7, 9-12, 23, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patel as applied to claims 13 and 25 respectively above, and further in view of Schneier ("Applied Cryptography").

Patel disclosed a system for efficiently generating pseudo-random bits in a computing environment, comprising: means for providing an input value; means for generating an output sequence of pseudo-random bits using the provided input value as an exponent of a 1-way function comprising modular exponentiation modulo a safe prime number wherein a length in bits, C, of the input value is substantially shorter than a length in bits, N, of the generated output sequence and a base of the modular exponentiation is a fixed generator value and means for using C selected bits of the generated output sequence as the provided input value for the next iteration of the means for generating while using all N-C remaining bits of the generated output sequence as pseudo-random output bits, until a desired number of pseudo-random output bits have been generated (See rejection of claim 13 above), but Patel failed to disclose that this system was implemented in software, and further failed to disclose that the input comprised non-contiguous bits of the previous output. However, Patel did disclose that these pseudo-random bits were for encryption (See Patel Page 305 Lines 15-17).

Schneier teaches that any encryption algorithm can be implemented in software and that doing so helps with flexibility and portability, ease of use, and ease of upgrade (See Schneier Page 225 Paragraph 7 Lines 1-3). Schneier further teaches that software encryption programs are popular (See Schneier Page 225 Paragraph 8 Line 1). Schneier also teaches that in order to reach a maximal period for a pseudo-random bit generator, the feedback bits should be a primitive polynomial mod 2 (See Schneier Page 374 lines 9-20, and further shows an example of this type of feedback (See Schneier Page 375 Figure 16.4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier to the pseudo-random bit generator of Patel, by implementing the generator in software, and by providing primitive polynomial mod 2 feedback to the generator. This would have been obvious because the ordinary person skilled in the art would have been motivated to improve the portability, ease of use, and ease of upgrade of the generator, and to provide the longest period for the generator to ensure the most produced bits before cycling.

Claims 2, 6-7, 9-10, and 12 are rejected for the same reasons as claim 14, 18-19, 21-22, and 24 above, as applied to claim 1.

Conclusion

Claims 1-7, 9-19, 21-32, 34-37, 39-45, and 47 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Patel et al. (U.S. Patent Number 6,285,761) disclosed a pseudo-random bit generator based on the assumption known as "discrete logarithms with short exponents".

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
8/3/2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100